Apple's Recent Lawsuit Against OpenAI Serves as a Reminder That Companies Must Be Vigilant in Protecting Their Trade Secrets

July 14, 2026

Source: *Saiber Employment Law Alert*

On July 10, 2026, Apple Inc. filed a lawsuit against OpenAI, two former Apple employees, and io Products, LLC, alleging a coordinated scheme to steal Apple's trade secrets.

The case is not only intriguing because of the heavyweight companies involved, but also because Apple's allegations should remind companies of every size that they must be vigilant in protecting their trade secrets and confidential information.

Apple has invested hundreds of billions of dollars and has cutting-edge technologies to protect its confidential information. If it can fall victim to misappropriation, no organization is immune. The Complaint serves as a reminder that companies should regularly audit their trade secret protections, particularly in connection with employee departures, hiring processes, and third-party relationships.

Summary of Apple's Allegations

Apple alleges that after OpenAI entered the consumer hardware market in late 2025, it systematically recruited Apple employees and extracted their knowledge of Apple's proprietary technologies. Specifically, Apple alleges:

- Defendant Chang Liu left Apple in January 2026. Apple alleges he failed to return an Apple-issued laptop, exploited an authentication vulnerability to access Apple's cloud-based file repository weeks after his departure, and downloaded dozens of confidential files while employed by OpenAI.

- Defendant Tang Yew Tan allegedly used Apple's internal project code names during OpenAI interviews, directed candidates to bring physical Apple components to interviews for "show and tell" sessions, and circulated an internal Apple document describing departure security procedures to help new hires evade Apple's protective measures.
-

  OpenAI allegedly structured its hiring process to extract confidential Apple information, instructing candidates to prepare "Technical Deep Dive" presentations using Apple's proprietary materials, and approached Apple's trusted suppliers using misappropriated knowledge to obtain proprietary manufacturing techniques.

If Apple Is Vulnerable, Every Company Is at Risk

Apple's Complaint details a very thorough corporate trade secret protection program. Apple requires all employees to sign Intellectual Property Agreements as a condition of employment. It uses need-to-know access controls, code names for projects, annual confidentiality training, locked buildings, security cameras, guards, and badge-restricted access. It imposes stringent confidentiality obligations on suppliers, maintains proprietary shipping processes for prototypes, and employs dedicated exit procedures for departing employees.

Despite this, Apple alleges its trade secrets were still compromised. The alleged misconduct does not involve sophisticated hacking. To the contrary, the primary allegations involve employees who did not return company-owned devices, who used private messaging apps to avoid detection, who coached departing employees on how to evade security checks and used insider knowledge to extract confidential information from Apple employees and suppliers.

What Can Companies Learn From the Complaint to Protect Their Own Trade Secrets?

1. **Strengthen and enforce trade secret protections, employee agreements, and departing employee procedures.** Trade secret protection is not "set it and forget it." Apple's Complaint reveals that even a company with industry-leading security can be blindsided by a previously unknown authentication bug, an unresponsive departing employee, or a supplier who is deceived into believing it has authorization to share confidential information. Trade secret protections must be continuously tested and updated.
2. **Tighten procedures for departing employees.** Like Apple, many companies require exit interviews, device return verification, and system access termination. But those procedures must be implemented, followed, and if a departing employee fails to return a company-owned device, or remains able to access the company's data, those breaches must be discovered and addressed promptly.
3. **Reinforce supplier and partner agreements.** Ensure that contracts with suppliers, vendors, and partners include explicit use restrictions, confidentiality obligations, and clear protocols for verifying authorization before performing work for third parties.
4. **Train employees on hiring-side risks.** If a company is hiring from competitors, it should ensure that interviewers do not solicit proprietary information from interviewees. These actions could expose the hiring company to liability.
5. **Document your protective measures.** Under the Defend Trade Secrets Act, a trade secret owner must demonstrate "reasonable measures" to maintain the secrecy of its trade secrets. Companies should maintain a clear record of all contractual, technical, and physical safeguards and update them regularly.

6.

Promptly investigate when red flags appear. Companies that delay investigating suspicious activity risk both losing evidence and undermining their ability to show they took reasonable steps to protect their trade secrets.

If you have any questions about this alert, please contact Jack Losinger of Saiber LLC's Employment & Labor Law practice group.

Summer Associate Preya Singh assisted in the preparation of this alert.